REMARKS

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 were pending at the time of the Office Action.

Claims 1, 12, 16, 22, 26, 31, 38, 40, 49, and 58 are amended.

Claim 21 is presently canceled.

Thus, claims 1-2, 4-17, 19-20, 22-27, 29-35, 38-41, 43-50, 52-58, and 60-61 remain pending.

In this response, filed with a Request for Continued Examination, applicants respectfully request reconsideration and allowance of subject application.

Response to Remarks

Applicants appreciate the Examiner's lengthy response to its previously submitted remarks.

Applicants wish to briefly clarify those remarks to clarify its position. In particular, applicants wish to respond to the Examiner's comment in the Office Action mailed October 5, 2007, that "Applicant's arguments that Fox does not teach delegation are contrary to what Applicant has admitted in prior arguments." (Office Action, Page 2, Paragraph 2 of "Response to the Amendment.) Applicants did not intend to contradict any of its previous remarks. Respectfully, applicants maintain that Fox does not teach ***secure, constrained*** delegation as recited in the pending claims. Applicant will briefly summarize and clarify its position.

Applicants assert that Fox teaches two forms of delegation: delegation controlled by the client which is not the same delegation as recited in the pending claims, or unconstrained

delegation. First, in Fox's client-controlled delegation, the client is involved in generating and/or decrypting every credential needed by the proxy to access resources on the client's behalf. This is underscored by the diagram included on Page 3 of the Office Action. Referring to Fox, the steps in the Figure are used "to set up a session key ***between the client*** and the service." (Fox, Section 2.3, Page 158, Column 1, Paragraph 1; emphasis added).

Fox makes clear that its client is directly involved in obtaining the service ticket the proxy uses in eventually accessing the service for the client. The Office Action shows Figure 1(d) of Fox that diagrams messages 10-16. (Office Action, 3; Fox, Section 2.3, Figure 1(d), Page 157). Fox indicates that messages 10-16 follow the form of messages 5-9. (Fox, Section 2.3, Page 158, Column 2, Paragraph 2 of Section 2.3). Reviewing Fox, it is clear that, in messages 5-9 (mirrored by messages 10-14) does not allow the proxy to securely obtain a service ticket without involving the client (all references are to Fox, Page 158, Columns 1 and 2, Numbered Paragraphs 5-9):

- Message 5/10 – "client must construct authenticator."
- Message 6/11 – "Note the forwarded message contains . . . the authenticator constructed by the client."
- Message 7/12 – "The TGS returns the proxy ticket and a session key for use between the client and the proxy, all encrypted with $K_{C,tgs}$, so that only the client can decrypt the message."
- Message 8/13 – "The ticket and key are forwarded verbatim to the client, which decrypts them using $K_{C,tgs}$ and extracts the [service credential]."

- Message 9/14 – "The client forwards the proxy ticket and a constructed authenticator to [the proxy]."(Fox At 10, the client directs the proxy, Charon, to obtain a service key.

Respectfully, in any form of secured delegation described by Fox in which the client does not divulge its authentication credentials, unless the client itself creates the authenticators to request the service credential for the client (messages 5/10), decrypts the service credential (messages 8/13, because in messages 7/12 the credential is presented in a form that only the client can decrypt); and then provides the credential to the proxy (messages 9/14), the proxy can do nothing. For this reason, as described further below, Fox fails to teach or suggest what is recited by the claims.

Second, the Office Action cited another portion of Fox for support that Fox's proxy, Charon, can negotiate for service credentials on its own behalf. However, what the Office Action fails to note is that the proxy can only negotiate for these credentials using dangerous, ***unconstrained*** delegation:

> An alternate approach that places more trust in Charon is for the client to reveal to Charon $K_{c,tgs}$ over the established secure channel, thus allowing Charon to negotiate for Kerberized services directly (since it can now construct the authenticators that must accompany the TGT on each request). ***In this case, Charon still doesn't have the user's Kerberos password, but because it has Kc,tgs, it can do more damage should it be compromised. Specifically, an attacker who controls Kc,tgs can impersonate the client's principal for the lifetime of the TGT, which is specified at the time the TGT is requested but in practice may be several hours.***

(Fox, Section 2.3, Page 158, Column 2, Last Paragraph through Page 159, Column 1, First Paragraph; emphasis added). Fox thus acknowledges that, if the client is not involved and the proxy is "trusted more," the delegation would facilitate attacks and potentially allow damage to the system.

Respectfully, neither of these irreconcilably different approaches teaches what is recited in the claims in constraining delegation while allowing a server to act on behalf of the client without continually involving the client. This is the point applicants sought to make in its remarks. Applicants apologize if its previously submitted remarks did not explain this with sufficient clarity.

Rejections under 35 U.S.C. § 102(b)

Respectfully, the rejections of claims 1-2, 4-17, 19-20, 22-27, 29-35, 38-41, 43-46, 48-50, 52-55, 57-58, and 60-61 under 35 U.S.C. § 102(b) must be withdrawn because Fox fails to teach or suggest the elements of the rejected claims.

The following discussion focuses on each of the independent claims, claims 1, 12, 16, 26, 31, 38, 40, 49, and 58.

Fox fails to teach or suggest the elements of claim 1 as amended. Claim 1 is reproduced below for the convenience of the Examiner:

> 1. (Currently Amended) A method for constraining delegation by a client to a server, comprising:
> a client obtaining a service credential to access a server from a trusted third party;
> authorizing the server to access one or more services on behalf of the client by one of:
> causing the service credential to specify that delegation of the service credential from the client to the server is authorized; and
> causing the trusted third party to maintain an indication that the delegation of the service credential from the client to the server is authorized;
> the client receiving the service credential from the trusted third party;
> the client providing the service credential to the server;
> the client requesting access to a resource through the server;

the server identifying for the client that the resource is provided by a target service that does not reside on the server ~~to which access is sought on behalf of a client~~;

the ~~causing a~~ server itself requesting ~~operatively coupled to the client to request~~ a new service credential to access the target service on behalf of the client from the ~~a~~ trusted third-party;

the client withholding from the server ~~without providing~~ a client's authentication credentials and capability to use the client's authentication credentials; ~~, wherein~~

the server providing ~~provides~~ the trusted third-party with:

a credential authenticating the server; and ~~,~~

I information about the target service; ~~,~~ and ~~a service credential previously provided by the client to the server allowing the client to access the server; and~~

causing the trusted third-party to provide ~~the server with~~ the new service credential that authorizes the server to access the target service on behalf of the client without participation by the client when one of:

the service credential specifies that delegation of the service credential to access the target service is authorized; and

the trusted third-party maintains an indication that the delegation of the service credential to access the target service is authorized.

Applicants submit that claim 1 is patentably distinct from Fox for at least five reasons. First, Fox teaches nothing about "the server identifying for the client that the resource is provided by a target service that does not reside on the server." In Fox, the client issues its request to access a specified proxy service through Fox's Charon. (Fox, Page 158, Column 1, Numbered Paragraph 5). In other words, Fox's proxy does not identify where the target service resides and arrange to obtain access to it as recited in claim 1; in Fox, the client initiates its own requests for service credentials, thus, the client must identify itself where to access the desired target service.

Second, Fox fails to teach or suggest "the server itself requesting a new service credential to access the target service on behalf of the client from a trusted third-party." Again, Fox describes a system in which it is the client that undertakes "[R]equest ticket for proxy service." (Fox, Page 158, Column 1, Numbered Paragraph 5). The Charon proxy does not do anything of

itself. As stated by Fox, "Charon ***relays*** the information to the TGS." (Fox, Page 158, Column 1, Numbered Paragraph 6; emphasis added). Thus, Fox fails to teach this limitation.

Third, Fox fails to teach or suggest "the client withholding from the server a client's authentication credentials and capability to use the client's authentication credentials." A previous Office Action, mailed January 4, 2007, that even though Fox recites that the proxy is provided with the client's authentication credential, the proxy cannot use the credential because the client withholds the password needed to use the credential, so the credential is effectively withheld from the proxy. However, as recited by claim 1 as amended, Fox does not teach both withholding the credential ***and*** the capability to use the credential. As a result, Fox fails to teach both aspects of this limitation.

Fourth, Fox fails to teach or suggest "causing the trusted third-party to provide the new service credential that authorizes the server to access the target service on behalf of the client without participation by the client." It is that Fox, except in an unconstrained implementation of Fox, requires the server to provide the new service credential client to decrypt the credential and pass it back to the server before the server can use it:

- "The TGS returns the proxy ticket and a session key for use between the client and the proxy, all encrypted with $K_{c,tgs}$, so that ***only the client can decrypt this message***."
- "The ticket and key are forwarded verbatim to the client, ***which decrypts them***."
- "The client forwards the proxy ticket and a constructed authenticator to Charon."

(Fox, Page 158, Columns 1-2, Numbered Paragraphs 7, 8, and 9; emphasis added). Fox fails to teach or suggest that the trusted third-party will provide a service credential to the server that the server can use without the participation of the client.

Fifth, Fox fails to teach "causing the trusted third-party to provide the new service credential" when "one of: the service credential specifies that delegation of the service credential to access the target service is authorized; and the trusted third-party maintains an indication that the delegation of the service credential to access the target service is authorized." As to this last point, the Office Action suggests that the delegability of the service credential is indicated by the service credential or by an indication maintained by the ticket-granting service is taught by Fox; respectfully, applicants are unable to determine how the cited portion of Fox, Section 2.3, Page 158, Column 2, Paragraphs 1-3, make such a teaching. In fact, according to Fox, whether a client "delegates" its authority is decided by the client on a case-by-case basis in determining whether to decrypt a service ticket and provide the service ticket to its proxy. Accordingly, Fox fails to teach this limitation.

In sum, Fox fails to teach all of the limitations recited by claim 1. Thus, the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 1.

Fox fails to teach or suggest the elements of claim 12 as amended. Claim 1 is reproduced below for the convenience of the Examiner:

> 12. (Currently Amended) A method for constraining delegation by a client to a server, comprising:
>
> a trusted third party providing a service credential to a client to access a server with delegation of authority by the client to the server to access one or more services signified by one of:
>
> marking the service credential as forwardable to the one or more services; and
>
> maintaining an indication that the server is authorized to access the one or more services on behalf of the client;
>
> the client providing the service credential to the server;
>
> the client requesting access to a resource through the server;
>
> the server identifying a target service not residing on the server to which access is sought on behalf of a client to obtain the resource; and
>
> ~~causing~~ the ~~a~~ server ~~operatively coupled to the client to request~~ requesting a new service credential to access to the target service on behalf of the client from

the trusted third-party without involving the client in the requesting of the new service credential ~~providing a client's authentication credentials~~, wherein the server provides the trusted third-party with an authentication credential authenticating the server, information about the target service, and the ~~a~~ service credential previously provided by the client to the server, and wherein the service credential previously provided by the client includes implementation-specific identity information constraining a scope of access delegated to the server; and

when the one or more services to which the delegation of authority by the client to the server includes the target service, causing the trusted third-party to provide the server ~~with a~~ the new service credential that authorizes the server without participation by the client to access the target service within the scope of access specified in the implementation-specific identity information.

Applicants submit that claim 12 is patentably distinct from Fox for at least four reasons. First, as previously described, Fox teaches nothing about "the server identifying a target service not residing on the server to which access is sought on behalf of a client to obtain the resource." Second, as also previously described, Fox fails to teach or suggest "the server requesting a new service credential to access to the target service on behalf of the client from the trusted third-party without involving the client in the requesting of the new service credential."

Third, again as previously described, Fox fails to teach or suggest "causing the trusted third-party to provide the server the new service credential that authorizes the server without participation of the client to access the target service within the scope of access specified in the implementation-specific identity information." The only support in Fox for the new service credential being provided to the server without the participation of the client involves unconstrained delegation in which the client provides its authentication credential and the capability to use that credential to the server. (Fox, Page 158, Column 2, Last Paragraph, through Page 159, Column 1, First Paragraph). However, as expressly Fox admits, providing these credentials to the proxy opens the system to attacks, and does not constrain the delegation. (Fox, Page 158, Column 2, Last Paragraph, through Page 159, Column 1, First Paragraph).

Thus, Fox fails to teach or suggest this limitation, restricting the access "within the scope of access specified in the implementation-specific identity information." Because Fox fails to teach these limitations, the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 12.

Fox fails to teach or suggest the elements of claim 16 as amended. Claim 1 is reproduced below for the convenience of the Examiner:

> 16. (Currently Amended) A computer-readable storage medium storing ~~having~~ computer-executable instructions for performing tasks for constraining delegation by a client to a server, comprising:
>
> in a server, determining a target service to which access is sought on behalf of a client coupled to the server; and
>
> in the server, requesting a new service credential from a trusted third-party to access the target service without participation of the client in processing the new service credential and without providing a client's authentication credentials by providing the trusted third-party with a credential authenticating the server, information about the target service, and a service credential that was previously provided to the client and the requesting server such that issuance of the new service credential authorizes the server to access the service on behalf of the client when one of:
>
> the service credential specifies that the service credential is delegable; and
>
> the trusted third-party maintains an indication that the service credential is delegable.

Applicants submit that claim 16 is patentably distinct from Fox for at least two reasons. First, again, Fox teaches nothing about "in the server, requesting a new service credential from a trusted third-party to access the target service without participation of the client in processing the new service credential." Second, Fox fails to teach or suggest "that issuance of the new service credential authorizes the server to access the service on behalf of the client when one of: the service credential specifies that the service credential is delegable; and the trusted third-party maintains an indication that the service credential is delegable." Again, in Fox, the client itself controls delegation by how it shares its credentials with the servers, and does not teach what

claim 16 recites to determine whether a credential is delegable. Fox fails to teach these limitations and the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 16.

Fox fails to teach or suggest the elements of claim 26 as amended. Claim 26 is reproduced below for the convenience of the Examiner:

> 26. (Currently Amended) A system comprising:
> a credential granting mechanism configured to:
> receive a request for a new service credential from a server and in response generate the new service credential granted in the name of a client rather than the server if delegation is allowable and without providing a client's authentication credentials and capability to use the authentication credentials, and wherein the request includes:
> a credential authenticating the requesting server,
> identifying information about a target service to which access is sought on behalf of the client coupled to the server, and
> a service credential that was previously granted to the client for use with the server; and
> grant the request and provide the new service credential to the server allowing the server to access the target service without participation of the client when the delegation is determined to be allowable by one of:
> the service credential presenting a forwardable delegation flag indicating the client has authorized the delegation to the target service as being within a scope delegated by the client; and
> the credential granting mechanism maintains an indication that the delegation to the server to access the target service is within the scope delegated by the client.

Applicants submit that claim 26 is patentably distinct from Fox for at least three reasons. First, in the context of constrained delegation as dictated by other limitations, Fox fails to teach or suggest how to "generate the new service credential granted in the name of a client rather than the server if delegation is allowable and without providing a client's authentication credentials and capability to use the authentication credentials." Second, Fox teaches nothing about how to "grant the request and provide the new service credential to the server allowing the server to access the target service without participation of the client." Third, Fox teaches nothing about delegation being "determined to be allowable when the delegation is determined to be allowable

by one of: the service credential presenting a forwardable delegation flag indicating the client has authorized the delegation to the target service as being within a scope delegated by the client; and the credential granting mechanism maintains an indication that the delegation to the server to access the target service is within the scope delegated by the client." Respectfully, Fox fails to teach these limitations. Thus, the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 26.

Fox fails to teach or suggest the elements of claim 31 as amended. Claim 31 is reproduced below for the convenience of the Examiner:

> 31. (Currently Amended) A system for constraining delegation by a client to a server, comprising:
> a server configured, on behalf of a client and without the participation of the client, to:
> determine that a request from the client seeks access to a resource provided by a target service;
> generate a request for a new service credential in the name of the ~~a~~ client rather than the server from a trusted third-party and to be issued to the server to allowing the server to access the target service without providing authentication credentials of the client and without the participation of the client, the new service credential being associated with a client and a target service, the request comprising:
> a credential authenticating the server,
> information about the target service, and
> a service credential associated with the client and the server
> wherein the server is allowed to access the target service when one of:
> the service credential specifies that the service credential is delegable; and
> the trusted third-party maintains an indication that the service credential is delegable.

Applicants submit that claim 31 is patentably distinct from Fox for at least four reasons. First, Fox teaches nothing about "a server configured, on behalf of a client and without the participation of the client, to: determine that a request from the client seeks access to a resource provided by a target service." Second, Fox fails to teach or suggest how to "generate a request

for a new service credential in the name of the a client rather than the server from a trusted third-party and to be issued to the server to allowing the server to access the target service without providing authentication credentials of the client and without the participation of the client." Third, Fox fails to teach or suggest the server being allowed to access the target service "when one of: the service credential specifies that the service credential is delegable; and the trusted third-party maintains an indication that the service credential is delegable." Fox fails to teach these limitations and the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 31.

Fox fails to teach or suggest the elements of claim 38 as amended. Claim 38 is reproduced below for the convenience of the Examiner:

> 38. (Currently Amended) A method comprising:
> separately authenticating a server and a client;
> providing the server with a server ticket granting ticket;
> providing the client with a client ticket granting ticket and a service ticket for use with the server;
> providing the server with the service ticket;
> in response to a request by the server, providing the server with a new service ticket for use by the server in accessing the new service for use with a new service without requiring the server to have access to content of the client ticket granting ticket and without the client participating in the request for the new service ticket when one of:
> the service ticket specifies that the service credential is delegable; and
> the trusted third-party maintains an indication that the service credential is delegable.

Applicants submit that claim 38 is patentably distinct from Fox for at least two reasons. First, Fox teaches nothing about "providing the server with a new service ticket for use by the server in accessing the new service for use with a new service without requiring the server to have access to content of the client ticket granting ticket and without the client participating in the request for the new service ticket." Second, Fox teaches nothing about issuing the new service ticket "when one of: the service ticket specifies that the service credential is delegable;

and the trusted third-party maintains an indication that the service credential is delegable." Again, Fox fails to teach these limitations. Accordingly, the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 38.

Fox fails to teach or suggest the elements of claim 40 as amended. Claim 40 is reproduced below for the convenience of the Examiner:

> 40. (Currently Amended) A method for constraining delegation by a client to a server, comprising:
>
> a server identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;
>
> causing the ~~a~~ server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication protocol method; and
>
> without participation of the client, causing the server to request from the second authentication method trusted third-party a new service credential for use by the server and the target service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with the credential authenticating the server, information about the target service, and the service credential to itself.

Applicants submit that claim 40 is patentably distinct from Fox for at least two reasons. First, Fox teaches nothing about "a server identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method." Second, Fox teaches nothing about "without participation of the client, causing the server to request from the second authentication method trusted third-party a new service credential for use by the server and the target service." Fox fails to teach these limitations, thus, the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 40.

Fox fails to teach or suggest the elements of claim 49 as amended. Claim 49 is reproduced below for the convenience of the Examiner:

49. (Currently Amended) A computer-readable storage medium storing having computer-executable instructions for performing tasks for constraining delegation by a client to a server, comprising:

a server identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;

causing the ~~a~~ server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service ticket to itself from a second authentication method trusted third-party by identifying the client and the first authentication method protocol;

causing the server to request a new service ticket configured for use by the server to access the new service without participation of the client ~~and~~ the identified service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with the credential authenticating the server to the client, information about the target service, and the service ticket to itself; and

causing the second authentication method trusted third-party to issue the new service ticket when one of:

the service ticket specifies the service ticket is delegable; and

the second authentication method trusted third-party maintains an indication that the service ticket is delegable.

Applicants submit that claim 49 is patentably distinct from Fox for at least four reasons. First, Fox teaches nothing about "the server identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method." Second, Fox teaches nothing about "causing the server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service ticket to itself." Third, Fox teaches nothing about "causing the second authentication method trusted third-party to issue the new service ticket allowing the server to access the new service without participation of the client." Fourth, Fox teaches nothing about the new service ticket being issued "when one of: the service ticket specifies the service ticket is delegable; and the second authentication method trusted third-party maintains an indication that the service ticket is delegable." Because Fox fails to teach any of these limitations, the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 49.

Fox fails to teach or suggest the elements of claim 58 as amended. Claim 58 is reproduced below for the convenience of the Examiner:

> 58. (Currently Amended) A system for constraining delegation by a client to a server, comprising:
>
> a server configurable to:
>
> identify a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method; ~~,~~
>
> use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication method, and
>
> subsequently request a new service credential, for use by the server independently of the client and the target service, from the second authentication method trusted third-party when one of:
>
> the service credential specifies the service credential is delegable; and
>
> the second authentication method trusted third-party maintains an indication that the service credential is delegable,
>
> wherein the server provides the second authentication method trusted third-party with the credential authenticating the server, information about the target service, and the service credential to itself.

Applicants submit that claim 58 is patentably distinct from Fox for at least four reasons. First, Fox teaches nothing about a server configurable to "identify a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method." Second, Fox teaches nothing about "use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication method." Third, Fox teaches nothing about configuring the server to "subsequently request a new service credential, for use by the server independently of the client." Fourth, Fox teaches nothing about a new service credential being issued "when one of: the service credential specifies the service credential is delegable; and the second authentication method trusted third-party maintains an indication that the service

credential is delegable. Fox again fails to teach these limitations, thus, the rejection under 35 U.S.C. § 102(b) must be withdrawn against claim 58.

Claims 2, 4-11, 13-15, 17, 19-20, 23-27, 29-30, 32-35, 39, 41, 43-46, 48, 50, 52-55, 57, and 60-61 depend from and apply additional limitations to the respective independent claims (and any intervening claims) from which each depends. Accordingly, these claims are allowable for at least the same reasons for which independent claims 1, 12, 16, 26, 31, 38, 40, 49, and 58 are allowable. Accordingly, the rejections under 35 U.S.C. § 102(b) must be withdrawn against claims 1-2, 4-17, 19-20, 22-27, 29-35, 38-41, 43-46, 48-50, 52-55, 57-58, and 60-61.

Rejections under 35 U.S.C. § 103(a)

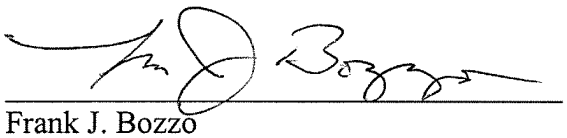
Claims 47 and 56 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Fox in view of Freier et al., "The SSL Protocol Version 3.0," November 18, 1996. Claims 47-56 depend from and apply additional limitations to independent claims 40 and 49, respectively, from which each depends. Accordingly, these claims are allowable for at least the same reasons for which independent claims 40and 49 are allowable. Accordingly, the rejections under 35 U.S.C. § 103(a) must be withdrawn against claims 47 and 56.

CONCLUSION

In view of the foregoing amendments and remarks, all pending claims are believed to be allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the applicants at the telephone number provided below.

Respectfully submitted,

MERCHANT & GOULD P.C.



Frank J. Bozzo
Registration No. 36,756
Direct Dial: 206.342.6294

MERCHANT & GOULD P.C.
P. O. Box 2903
Minneapolis, Minnesota 55402-0903
206.342.6200

27488
PATENT TRADEMARK OFFICE